Advances in Social Science, Education and Humanities Research, volume 273
International Conference on Communicative Strategies of Information Society (CSIS 2018)

Information and Economic Aspects of the Cryptocurrency Analysis

O.P. Sushko
Northern (Arctic) Federal University
Department of Economics and Entrepreneurship
Arkhangelsk, Russia
o.sushko@narfu.ru

A.A. Kaznin
Northern (Arctic) Federal University
Department of Applied Informatics
Arkhangelsk, Russia
a.kaznin@narfu.ru

***Abstract* - The paper considers the IT element of the global innovative economy, i.e. a blockchain. It demonstrates some results of SWOT analysis and PEST analysis of the cryptomarket, analysis of blockchain technologies used to create the digital currency and the market of digital currencies. It gives the analysis of cryptomarket capitalization and the currency rate dynamics.**

Keywords* - *cryptomarket, blockchain technology, statistical sampling, cryptocurrency rate dynamics, market capitalization, transaction, blockchain

I. INTRODUCTION

In general, the financial market is transforming rapidly under the influence of innovative digital technologies able to change many processes of the global community. The relevance of the given study is caused by active use of a new payment product – cryptocurrency, which at the same time serves the source of mixed attitude of authorities due to insufficient knowledge and uncontrollability of the digital currency market. State authorities try to operate and control cryptocurrency transactions, however its structure does not allow doing so since the digital currency has no central governing body, and hence the government cannot directly operate it and dictate certain rules and standards. State authorities of many countries are experiencing the outflow of money to the cryptocurrency market and are thus losing tax payments to the budget due to lack of taxation on cryptocurrency transactions. Hence, they try to tighten the regulations regarding the turnover of digital currency as much as possible. Thus, China is going to forbid foreign cryptocurrency exchange in the country [1, 22]. Indian authorities want to make cryptocurrency completely illegal. South Korea imposes restrictions on cryptocurrency trade in the registration procedure via the bank account. Since January 2018 the USA has been applying the tax on all cryptocurrency transactions [21]. The European Union and Australia also take a lot of regulatory efforts in their countries. Seeing a huge potential in the development of cryptocurrency some countries are trying to take the leading positions in this field. The president of Belarus signed the Decree On the Development of Digital Economy thus making it possible to legalize mining and transactions with tokens [3]. Venezuela was able to earn hundreds of millions of dollars on Petro cryptocurrency and plans to issue Petro Gold cryptocurrency [22]. This demonstrates that understanding the inevitability and activization of new IT processes the world central banks and public organizations [6, 13] are trying to regulate and operate the cryptocurrency market by developing methods and tools to influence the digital currency instead of banning it, and hence initiate the large-scale study of the matter. The cryptocurrency market will be subject to regulation and change, however the digital currency became an integral part of modern global community.

II. RESEARCH METHODS

The purpose of the current and future study of this matter includes the multi-criteria analysis of cryptocurrency within modern information economy. The object of the study includes cryptocurrency-based payment systems. The subject of the study covers theoretical and practical aspects of cryptocurrency payment systems. The initial stage of the study was based on the analysis of digital currency and assessment of cryptocurrency development in retrospective, issues of cryptocurrency protection against fraud. The next stage, which is still ongoing, includes the monitoring of cryptocurrency cost with further database creation, SWOT and PEST cryptocurrency analyses, the analysis of cryptocurrency market capitalization, factors of cryptocurrency market development, hash algorithms within the system of digital currency issue, influence of dedicated devices for technical mining on the development of cryptocurrency system, identification of problems and prospects of its development. The given work shows some results of the cryptocurrency analysis as means of payment and cryptocurrency-based payment systems.

III. LITERATURE REVIEW

The world universities and leading research centers are studying theoretical and practical aspects of digital economy, Blockchain technology and cryptocurrency [17, 18, 22]. Thus, in 2017 several scientific works devoted to cryptocurrency were published by the University of Cambridge. In 2016, the Cambridge Centre for Alternative Finance of the University of Cambridge (CCAF) held four online polls under the supervision of the research fellow G. Hileman, which resulted in the Global Cryptocurrency Benchmarking Study published in 2017, which was based on the analysis of data obtained from 51 exchanges in 27 countries of the world [19, 22]. The study shows that 85% of exchanges of the Asia-Pacific have no licenses, only one third of large exchanges and slightly more than a half of small exchanges of the European Union have the state license. North American exchanges demonstrate a more

positive situation in licensing (78%). The analysts highly appreciated the complex CCAF report on the state of affairs in the field of digital money.

Though cryptocurrency is based on the Blockchain technology and has relatively sufficient protection against fraud, the insufficient study of security regarding cryptocurrency leads to the fact that the majority of emerging applications, including mobile ones, fail to ensure satisfactory security. It is almost impossible to forge cryptocurrency as such (although possible, for example, in cryptocurrency mining the malefactors were able to change the blockchain, but after such attacks changes are immediately made to the algorithms of the corresponding platform) [4]. In 2017, the High-Tech Bridge (San Francisco) studied the cryptocurrency security within Google Play and revealed problems in all applications. The report "How secure are the most popular crypto currencies mobile apps" divides all user risks into four categories: High, Medium, Warning, Low. The main conclusions of the High-Tech Bridge are as follows [19]:

1. Insufficient cryptography.
2. Improper platform usage.
3. Insecure data storage.

In 2016, J. Poon and T. Dryja published a report "The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments", where they discovered that the Bitcoin Lightning network represents the expansion of bilateral channels regarding payments to ensure fast transactions between any number of participants [20].

The Committee on Payments and Market Infrastructures (CPMI) of the Bank for International Settlements studies security and efficiency of payment, clearing, settlement and related mechanisms, and publishes reports on innovations in retail payments and non-bank retail payments. The last report presents the study of decentralized digital currency.

Today large-scale studies of Blockchain technology are conducted by the financial and technological research consortium R3 (R3 CEV LLC) with its headquarters in the USA, which includes over 70 largest financial organizations and banks. In 2016, the consortium published the Corda project with the new blockchain technology (the protocol has no built-in cryptocurrency, only project participants can get access to the data) – a "distributed database designed for financial services" presented in the R3 Reports with Chain That report [6, 13].

In 2017, the Financial University under the Government of the Russian Federation conducted a study of cryptocurrency and Blockchain technology by the order of the State Duma of the Russian Federation [5, 16]. The results of the study will be used to create and design the package of legislative initiatives to regulate the cryptocurrencies of financial institutions.

Besides, there are some works on individual matters of digital currency. Experts in cryptocurrency, economy and other disciplines participate in the study. It shall be noted that the researchers make quite controversial conclusions using the same facts and data of market development, and to understand whether there is a need to accept or reject analytical results and opinions, there is a need to consider the objectives and tasks, research methodology, obtained results and their interpretation.

IV. PRELIMINARY FINDINGS

Technical and information aspect of the study

The cryptocurrency appeared in 2008-2009 to make money protected and independent of states though the cryptography appeared much earlier (in 1990) and was designed to ensure confidentiality of transactions in the centralized system (DigCash system) [7, 14]. According to experts and analysts of cryptocurrency market, the extensive use of blockchain technology will lead to major changes in IT world, i.e. the Blockchain technology [10, 11] based on distributed network of economic transactions using cryptography still remains the main driver of the digital currency market, which does not allow changing chains of blocks and saving them in file without the user keys. It also guarantees synchronization of copies of the distributed blockchain. Transactions are made by transferring the private user keys thereby transferring the sum of money stored in the corresponding section of a blockchain.

Each cryptocurrency uses a certain cryptography algorithm representing a hash function. The hash function is used to solve mathematical problems in case new blocks are embedded into the cryptocurrency network. Different hash algorithms are used in cryptocurrency networks, some of which may refer to 'cold', while the others to 'hot' algorithms. Cold algorithms (for example, CryptoNight or Lyra2Rev2) are thus called due to relatively small power consumption and, hence, smaller heating of the mining equipment, and hot algorithms (for example, Equihash) – vice versa. Table 1 shows the main hash algorithms and their corresponding cryptocurrencies.

TABLE I. TABLE STYLES

Hash algorithm	Brief description	Type of cryptocurrency
SHA-256 (Secure Hash Algorithm)	Hash function to create a 256-bit hash. Used for mining of the most popular cryptocurrency – Bitcoin. Fairly simple for mining, which resulted in the use of ASIC devices (application-specific integrated circuit) [21] in mining	Bitcoin (BTC), BitcoinCash(BCH), DGB-SHA(DGB)
Scrypt	Created by the Litecoin team for CPU and GPU mining only, however the ASIC devices were designed later for this purpose	Litecoin(LTC), Dogecoin(DOGE), Verge-Scrypt(XVG), Florin(FLO)
NeoScrypt	Created for Feathercoin cryptocurrency after the appearance of ASIC devices for the Scrypt algorithm. The main difference of the Neoscrypt algorithm is the restriction for the amount of remuneration for the received block for all types of cryptocurrencies thus created (from 60 to 90 cryptocoins)	Feathercoin(FTC), Trezarcoin(TZC), Phoenixcoin(PXC), Vivo(VIVO)
Ethash (DaggerHashimoto)	Developed for Ethereum cryptocurrency mining. Has high requirements to hardware. In 2018, ASIC devices for mining were designed on this algorithm. The software for GPU was developed, which provides for parallel mining of other cryptocurrencies based on Ethash algorithm (Decred, Siacoin, Lbry, Pascal, Blake2s, Keccak) during cryptocurrency mining based on the given algorithm	Pirl(PIRL), Ubiq(UBQ), Metaverse(ETP), EthereumClassic(ETC), Musicoin(MUSIC), Ethereum(ETH), Dubaicoin(DBIX), Ellaism(ELLA), Expanse(EXP)
Equihash	The mining algorithm Equihash is developed to exclude ASIC devices from mining by increasing requirements to memory resources. However, the taken measures failed to protect against ASIC devices, but later such measures were developed	Hush(HUSH), Zcash(ZEC), Zclassic(ZCL)
Zhash	Further development of Equihash algorithm with the corresponding ASIC devices. This made it possible to exclude ASIC devices from cryptocurrency mining	BitcoinGold(BTG), BitcoinZ (BTCZ)
CryptoNight	CryptoNight algorithm is characterized by high degree of confidentiality. Initially the algorithm showed good calculation results on CPU. Now ASIC devices, which do not allow applying CPU and GPU to mining, are produced	Electroneum (ETN), Karbo (KRB), Sumokoin (SUMO)
CryptoNightV7	CryptonightV7 algorithm represents a new algorithm, which is resistant to ASIC devices. It was created after Hard Fork [22] in the network of Monero cryptocurrency (XMR) after the development of ASIC devices for the previous algorithm of this coin – CryptoNight	Monero(XMR), Graft(GRFT), DigitalNote(XDN)
CryptoNightHeavy	It was developed to create the algorithm resistant to ASIC devices after their appearance on the basis of CryptoNight algorithm	Ryo(RYO), Loki(LOKI)
Lyra2REv2	The important feature of Lyra2REv2 algorithm is adjustment of time and memory parameters for mining. When ASIC devices appear for mining the memory intensity will be changed thus making ASIC devices useless	Vertcoin(VTC), Straks(STAK), Verge-Lyra2REv2(XVG)
X11	X11 algorithm has high degree of security with 11-round system (11 hash functions)	Dash(DASH), Paccoin($PAC)

Economic aspect of the study

The methods of elementary analysis of cryptocurrency exchange rates and one-dimensional statistical tests were used prior to the regression analysis. The regression analysis of retrospective development of different types is cryptocurrency throughout a long period showed that their dynamics is free from any long-standing regular stochastic changes (Fig. 1-3). The wavelength has no similar time bounds thus indicating the lack of recurrence. Seasonal changes were not revealed in the dynamics of cryptocurrencies. A positive tendency is observed as a result of the regression analysis of price dynamics of cryptocurrencies from 2010 - 2014 (depending on the appearance of cryptocurrencies at exchanges) [8, 9, 16] until present. A relatively stable price tendency after 2014 demonstrates active development of the cryptocurrency market influenced by a variety of continuous and a number of insignificant short-term factors.

The important aspect of price dynamics of different cryptocurrencies is their similar positive linear correlation confirmed by the correlation analysis demonstrating the influence of similar factors. According to the Pearson linear correlation, the design ratios of price dynamics of cryptocurrencies vary within 0.89-0.98. Since the correlation ratios are calculated by finite sampling, the importance of correlation ratios is defined via t-criterion. The absolute t-criterion is not less than the critical t, therefore the experimental data with 0.9 probability (1 - α), do not contradict the hypothesis concerning the dependence of random variables of cryptocurrencies.

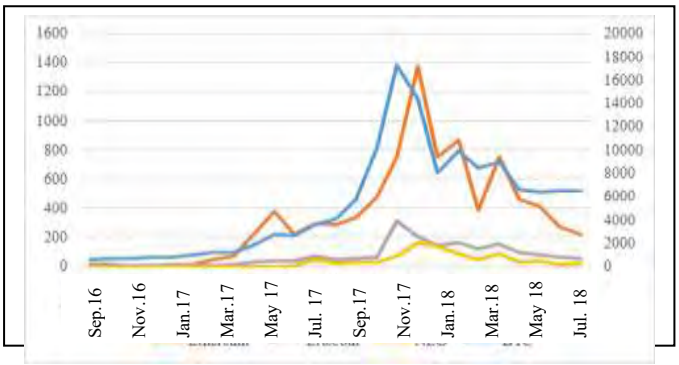

Fig. 1. Cryptocurrency dynamics *(according to Coinmarketcap).*

Despite a large number of cryptocurrencies (over 2000 these days) the Bitcoin remains the all-time leader holding 55% of the market. Though it shall be noted that at the

beginning of 2018 the bitcoin capitalization reached its record low (34% of the total cryptocurrency market) in its entire ten-year history, which was caused by the mistrust of investors and transfer of assets to other types of cryptocurrencies. Some types of altcoins are gaining their popularity (all other cryptocurrencies are considered altcoins) [9, 14]. According to Coinmarketcap [8, 12], as of September 2018 all cryptocurrencies were roughly ranked as follows: Bitcoin, Ethereum (11% of capitalization market), Ripple (6%), Bitcoin Cash (4%), Litecoin, Dash, NEO, IOTA, Monero, NEM.

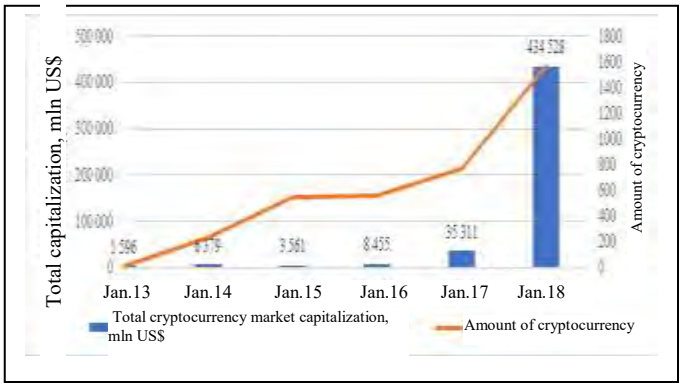

Fig. 2. Cryptocurrency dynamics *(according to Coinmarketcap).*

At present, the cryptocurrency exchange trade is also gaining popularity. It unites sellers and buyers of cryptocurrencies and traditional world money. Exchange platforms are similar to standard exchanges, which automate purchase and sale of currency pairs, and settle quotations. Until 2014 over 70% of the trading volume was done at the Mt. Gox exchange, but with the trading halt at the beginning of 2014, the cryptocurrency market faced the crash of its quotations by almost 80% [1]. This set the stage for new Internet trade associations, and now trade is distributed through various platforms with at least 10% of the trading volume [1]. Currently, there are two key players in the market (Coinbase and its division GDax) – leaders on fund raising into the ecosystem [15].

The major *factors* determining the cost of *cryptocurrencies* include the supply-demand balance, cost of energy, production technology and its complexity, government policy [9, 14]. Besides, there are other minor factors influencing the cryptocurrency cost. It is worth mentioning here the investments, which considerable volume result in the fact that the cost of cryptocurrencies will be increasing, and even considering all risks and volatility the digital means of payment will present an interest to investors.

Now some cryptocurrency miners are confined to mining profitability and the demanding requirements to equipment and energy consumption [5, 11].

V. Conclusions

Cryptocurrency is quite promising for a modern global community, but now, it inspires a little trust since information technologies for cryptocurrency creation and circulation are passing through intense competition with traditional payment services (cash and non-cash money) thus making the users uncertain in their position and choice. Besides, mistrust to cryptocurrency there is a problem with the legislation since public authorities and banks are not able to control money turnover, which may become an obstacle for further development of digital currency [11]. Lack of control over daily cryptocurrency circulation jeopardize the existence of states as they do today. Cryptocurrency is not tied to one country of the world; its universality breaks economic boundaries between states. Neither country is able to exist without finances and taxes. In this regard, the majority of the world countries are concerned with rapid development of cryptocurrencies and are already creating the legal framework in this field. Despite attempts of the states to settle the creation and exchange of cryptocurrency, it has sufficient opportunities for further growth [10, 16].

The results of the study show that the cryptocurrency market is very unstable due to infancy of the market and lack of regulatory mechanisms. The pop-up cryptocurrency market grows rapidly without any legislative framework both at the level of certain states and the world in general. The Blockchain technology with its high potential not only in the economic sector but also in many other areas of society remains the main driver for the development of digital currency market. There are various types of cryptocurrencies at present, some of which are not used in circulation, new types are created, which also demonstrates the lack of regulating tools, methods, standards, as well as the development of the digital currency market.

ASIC devices exert a great influence on the development of cryptocurrencies. The analysis of cryptoalgorithms shows that the network protection with cryptocurrency against ASIC devices is one of the most important tasks that the cryptocurrency developers face these days. ASIC devices are quite powerful and compact. This allows concentrating big capacities of a cryptocurrency network in one place, which poses a huge threat to decentralization and security of cryptocurrency networks.

The analysis of information security showed that it is critical to ensure stability of cryptocurrency systems against potential changes to a blockchain (mainly, it concerns new cryptocurrencies with a relatively small network power). Besides, it is important to pay more attention to information security when dealing with cryptocurrencies.

It is complicated to analyze the future of unstable cryptocurrency market since the situation depends on a number of factors and conditions. In many respects, the medium and long-term development of the cryptocurrency market will depend on governmental decisions, broader economic context, development of digital technologies and technical enhancement. The very idea of independent means of online payment is still relevant.

The results of the study make it possible to note that during the present period of active development of the cryptocurrency market under adverse international situation for Russia there is a need to utilize scientific and technological digital payment processes for early recovery of competitive positions. How shall a state ensure taxation and control money turnover both from technical and economic perspective? So far, this question remains open. This task cannot be solved without further study of information, technical and economic aspects. In this regard, the future study of this relevant topic will include the detailed

factorial analysis, trend design, forecasting of cryptocurrency for different periods, analysis of information and technical aspects of cryptocurrencies and design of data mechanisms to handle them.

References

[1] N.V. Apatov, O.L. Korolev, A.P. Krulikovsky, "Analysis of the influence of blockchain technology on financial system", Scientific and technical bulletin of St. Petersburg State Polytechnic University, Economic sciences, 2017, vol. 10, No. 6, pp. 31-39.

[2] N.V. Boss, N.M. Rubtsov, "Cryptocurrency as an element of financial system of the modern world", Scientific idea, 2017, vol. 3 (3), pp. 37-45.

[3] Belarus legalized the mining of cryptocurrencies [Electronic resource] URL:https://www.rbc.ru/finances/22/12/2017/5a3cf1b79a79470ff47031fe.

[4] S.B. Veprev, V.A. Perov, "Questions of information security in case of cryptocurrency", Bulletin of the Russian New University, Series: Complex systems: models, analysis and management, 2017, vol. 2, pp. 66-68.

[5] M.E. Mezina, O.Ya. Starkova, "Cryptocurrency: state and prospects of development in Russia, In the collection: Economic sciences", Current state and prospects of development, pp. 135-138 [Proceedings of the XI international students' scientific and practical conference, 2018].

[6] N.M. Korotkova, "Cryptocurrency in Russian economy: prospect or threat to security, In the collection: Science. Technologies. Innovations", Collection of scientific works: in 10 parts, 2017, pp. 211-214.

[7] A.A. Krylov, D.V. Milyutin, "Cryptocurrency bitcoin - a new form of financial interaction: basic principles of work and threat to economic security", Microeconomics, 2017, vol. 6, pp. 95-100.

[8] Current exchange rate [Electronic resource] URL:https://www.sberometer.ru/bitcoin.php/.

[9] Exchange rate of the dollar [Electronic resource]. URL:https://www.fxclub.org/markets/crypto/.

[10] A.V. Ponkratova, R.A. Sarkisova, K.A. Avanesyan, "Blockchain and prospects of its use in financial organizations", Social sciences, 2017, vol. 4 (19), pp. 135-140.

[11] Problems of the world of cryptocurrency and their complex solution [Electronic resource]. URL:https://geektimes.ru/company/xronos/blog/292769/ (date of access: 31.09.2018).

[12] S.A. Filin, L.A. Chaykovskaya, "Cryptocurrency: features of regulation, possibilities of accounting and taxation", Economy and management: problems, solutions, 2018, vol. 1 (3), pp. 65-79.

[13] E. Shavina, O. Kalenov, S. Kukushkin, cryptocurrency to become S. Can cryptocurrency become an alternative to traditional currencies? Economy of knowledge: theory and practice, 2017, No. 4, pp. 93-95.

[14] A.V. Shokarev, R.A. "Smirnov, Implication and main advantages of bitcoin trading", In the collection: mechanisms of economic system management: methods, models, technologies, pp. 245-248 [Collection of articles of the International scientific and practical conference, 2017]

[15] D.S. Shchegolkov, "Possibility of using the blockchain technology and cryptocurrency in modern economy", Central scientific bulletin, 2017, vol. 2, No. 23s (40s), pp. 58-60.

[16] Bitcoin [Electronic resource] URL:https://bitcoin.org/en/glossary/hard-fork.

[17] Cambridge Centre for Alternative Finance, "Global Cryptocurrency Benchmarking Study", 2017, [Electronic resource] URL: https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative finance/downloads/2017-global-cryptocurrency-benchmarking-study.pdf.

[18] Cointelegraph. How Blockchain Technology Works. [Electronic resource], URL: https://cointelegraph.com/bitcoin-for-beginners/how-blockchain-technology-works-guide-for beginners#hash-function

[19] How secure are the most popular cryptocurrencies mobile apps? 2017 [Electronic resource] URL: https://www.htbridge.com/

[20] J. Poo, Th. Dryja "The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments", 2016 [Electronic resource] URL: https://lightning.network/lightning-network-paper.pdf.

[21] L! FE. Donald Trump signed the bill of amendments to the US Tax Code. Since New year all transactions with cryptocurrency will be taxed. [Electronic resource]. URL:https://life.ru/t/%D0%B1%D0%B8%D0%B7%D0%BD%D0%B5%D1%81/1074395/ssha_vvieli_nalogh_na_kriptovaliuty_no_nikto_nie_ispughalsia.

[22] R3 Reports with Chain That, 2017, URL: https://www.r3.com/research/